IT Policies

Comhairle Ceantair an Iúir, Mhúrn agus an Dúin
Newry, Mourne and Down District Council

Policy Control

Policy reference:	CS8
Title of Policy:	IT Policies
Version:	1.1
Directorate / Departmental ownership:	Corporate Services/Digital and Communications
Officer responsible:	Assistant Director – Digital and Communications
Date of ratification:	01/02/2015
Review date:	18/12/2025
Equality screening and Rural Needs Impact Assessment completed by:	Gavin Ringland (IT Manager)
Equality screening and Rural Needs Impact Assessment date:	02/06/2025
Location where document is held and referenced:	Responsible Department ☒ Corporate Policy repository ☒

Revision History

Version	**Originator**	**Review Start Date**	**Revision description and record of change**
1.0	Gavin Ringland	29/07/2025	Approved by SMT on 29/07/2025.
1.1	Gavin Ringland	18/12/2025	Addition of Microsoft 365 Policy. Approved by SMT on 18/12/2025.

Contents

Related policies and legislation

Supporting procedures, policies, and guidelines

Supporting procedures have been developed to strengthen and reinforce these policies. These, along with associated policies and guidelines are published together and are available for viewing on the Council Intranet. Printed copies can be obtained upon request.

All staff, users, and any third parties authorised to access the Council' network or IT facilities are required to familiarise themselves with these supporting documents and to adhere to them.

Relevant legislation

The Council has a responsibility to abide by and adhere to all current Northern Ireland, UK and EU legislation as well as a variety of regulatory and contractual requirements.

A non-exhaustive summary of the legislation and regulatory obligations that contribute to the form and content of this policy is provided below.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the summarised legislation.

Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:

1. unauthorised access to computer material
2. unauthorised access with intent to commit or facilitate commission of further offences
3. unauthorised modification of computer material

The Data Protection Act

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently

- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Freedom of Information Act 2000

The Freedom of Information Act 2000 makes provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act (Northern Ireland) 2022

"Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm."

Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

Children Order (Northern Ireland) 1995

The Children Order (Northern Ireland) 1995, provides the legislative framework that governs the response to, and services provided for, children in need of support, at risk of harm and for those who have suffered abuse and harm.

Definitions

Availability	Property of being accessible and usable upon demand by an authorised entity.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Council	Newry, Mourne and Down District Council is a Northern Ireland Local Authority with its registered office at O'Hagan House, Monaghan Row, Newry, Co. Down, N. Ireland, BT35 8DJ.
Cryptographic	The practice of securing information and communication through the use of codes, ensuring that only the intended recipient can access and understand the information.
Data	Information in raw form.
Information	The result of processing, manipulating, or organising data. Examples including but not limited to; text, images, sounds, codes, computer programmes, software, and databases.
Integrity	Property of accuracy and completeness.
Patch	A software update designed as an interim measure between version releases to change functionality, usually to fix a specific problem.
Relevant legislation	A non-exhaustive summary of the legislation and regulatory obligations that contribute to the form and content of this policy/procedure.
Sensitive information	All information classified as private, confidential or highly confidential.
Staff	Staff are employees, elected members, or individuals contracted to Council to provide a service.
Visitor	A visitor is anyone, not a member of staff, requiring access to Council premises or services.

This document uses the following terms.

- 'We', 'us' and 'our' when referring to the Council (as an organisation), our collective responsibilities (as authorised users of council IT assets), and when discussing specific activities.
- 'You' and 'your' when referring to the individual responsibilities and actions of authorised users of Council IT assets.

Department and Officer responsible

Directorate / Department	Corporate Services/Digital and Communications
Officer(s) responsible for developing the policy	IT Manager

Policy approval process

Meeting	Date
CMT	N/A
SMT	18th December 2025
Finance and Resources Committee	7th January 2015
Monthly Council Meeting	1st February 2015

Review date

These policies, and supporting documentation, shall be reviewed and updated in line with the Council's agreed policy review cycle i.e. every 4 years (as per Council's Equality Scheme commitment 4.31), or more frequently when best practice or the legislative/regulatory environment changes, to ensure that they:

- remain operationally fit for purpose
- reflect changes in technologies
- are aligned to industry best practice
- support continued regulatory, contractual and legal compliance.

Procedures and arrangements for monitoring the implementation and impact of the policy

The Council shall conduct security, compliance and assurance activities, facilitated by Council staff and associated service providers to ensure security objectives and the requirements of the policies are met. Wilful failure to comply with the policies will be treated extremely seriously by the Council and may result in enforcement action on a group and/or an individual. If you have any questions or concerns about these policies, please discuss them with your line manager.

Enforcement actions may include:

- restrictions on access to Council digital resources, including email and Internet
- requirement to complete or repeat training
- restrictions on ability to work away from the office
- escalation to Council management.

Equality screening

These policies have been screened, and the decision made that they are not subject to an EQIA (with no mitigating measures required).

Rural Needs Impact Assessment

These policies have been assessed for impact against rural needs.

Acceptable use

Outlines the Council’s approach to acceptable use of its computing facilities.

Statement

This policy outlines the Council’s approach to acceptable use of its computing facilities and provides the guiding principles and responsibilities to ensure the Council’s acceptable use objectives are met.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Access control

Outlines the Council’s approach to access control of its computing facilities.

Statement

This policy outlines the Council’s approach to access control of its computing facilities. It provides the guiding principles and responsibilities to ensure the Council’s access control objectives are met.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- access to ‘OFFICIAL’ data/information is governed by this policy.

There are no restrictions on access to ‘PUBLIC’ information.

The policy will be communicated to users and relevant external parties.

AntiVirus/Malware

Outlines the Council’s approach to anti-virus/malware protection for its computing facilities.

Statement

This policy outlines the Council’s approach to anti-virus/malware protection for its computing facilities and provides the guiding principles and responsibilities to ensure the Council’s anti-virus/malware objectives are met.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Asset management

Outlines the Council’s approach to management of its information technology assets.

Statement

This policy outlines the Council’s approach to management of its information technology assets and provides the guiding principles and responsibilities to ensure the Council’s asset management objectives are met.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Backup verification and recovery

Outlines the Council’s approach to data backup, verification and recovery.

Statement

This policy outlines the Council’s approach to data and system backup, verification and recovery and provides the guiding principles and responsibilities to ensure the Council provides a means of recovering data or a system to a known state or point in time.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- identify and establish processes, procedures and good working practices for the backup and timely recovery of the Council’s information and data existing in electronic form
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Change management

Not yet applicable/developed.

Clear desk

Refer to the Council Records Management Policy and Procedure.

Client device

Key policy facts, responsibilities, and processes in relation to the management of client devices for Council employees.

Statement

This policy covers the selection, purchase, deployment and disposal of physical desktop and laptop computers by the Council on behalf of its staff.

Aim

This policy aims to minimise the costs and risks inherent in purchasing and supporting a large estate of IT equipment by a diverse user group.

Scope

This policy applies to all PCs and non-PC computers (desktop or laptop) running Windows, purchased using Council funds for staff in their normal duties. Client devices supplied, through or funded, by the Council are for the business of the organisation and remain the property of the Council unless an externally funded grant explicitly states that the device can move with the member of staff.

The policy excludes:

- devices covered by the IT Mobile and Bring Your Own Device (BYOD) policy
- specialised servers, storage and core infrastructure purchased by Council IT, which are subject to separate standards
- specialised, single use, client equipment (e.g. embedded PCs or clients connected to equipment such as a kiosks).

Cryptographic

Not yet applicable/developed.

Cyber vulnerability management

Outlines the Council's approach to cyber vulnerability management.

Statement

The purpose of the Council Cyber vulnerability management policy is to establish a structured and systematic approach to identification, assessment, prioritisation, and remediation of security vulnerabilities within its information technology (IT) infrastructure. This policy plays a crucial role in the Council's overall cybersecurity strategy and aims to enhance its ability to maintain a secure and resilient IT environment.

Aim

The Council's objectives for this policy are to:

- safeguard the Council's information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects
- instil a culture which actively encourages effective management of cyber vulnerabilities.

Scope

This policy applies to:

- All systems and services which connect to the Council network.

The policy will be communicated to users and relevant external parties.

Data classification

Refer to the Council Records Management Policy and Procedure.

Data handling

Refer to the Council Records Management Policy and Procedure.

Data movement/transfer

Refer to the Council Records Management Policy and Procedure.

Data retention

Refer to the Council Records Management Policy and Procedure.

Disposal of all Waste Electronic and Electrical Equipment

Refer to the Council Waste Management Policy.

Electronic messaging

Outlines the Council’s approach to use of electronic messaging facilities.

Statement

This policy outlines the Council’s approach to use of electronic messaging facilities. It provides the guiding principles and responsibilities to ensure the Council’s electronic messaging objectives are met.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Incident management

Outlines the Council's approach to IT incident management.

Statement

The purpose of the Council Incident management policy is to establish a structured and systematic approach to IT incident management, fostering a culture of proactive incident reporting and logging to help reduce the number of security incidents, ensuring at all times that any incident which could cause damage to the Council's assets and reputation, or which could adversely impact an individual's rights or freedoms, is prevented and/or minimised.

Aim

The Council's objectives for this policy are to:

- safeguard the Council's information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects
- instil a culture which actively encourages effective management of cyber vulnerabilities.

Scope

This policy applies to:

- All systems and services which connect to the Council network.

The policy will be communicated to users and relevant external parties.

Information security awareness

Outlines the Council's approach to information security awareness.

Statement

This policy states the Council's approach to information security awareness. It describes the guiding principles and the responsibilities needed to meet the Council's information security awareness objectives.

Aim

The Council's objectives for this policy are to:

- safeguard the Council's information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects
- instil a culture which actively encourages the knowledge and effective use of cyber and information security best practices amongst staff
- ensure that all staff understand and comply with the information security practices required of them by the Council.

Scope

This policy applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information.

The policy will be communicated to users and relevant external parties.

Information security

Outlines the Council’s approach to information security management.

Introduction

Information, in all its forms, is a primary asset and the lifeblood of the Council; its effective curation and protection is critical to maintaining the Council’s operational effectiveness, financial viability and reputation.

Aim

The objectives of this policy are to:

- safeguard the Council’s information from both internal and external security threats that could have an adverse effect on its operations, financial position or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects
- ensure that all users of the Council’s information understand their roles and responsibilities in relation to information security.

Scope

This policy is applicable to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Microsoft 365

Outlines the Council's approach to use of Microsoft 365.

Statement

This policy recognises that the Microsoft 365 is a rapidly evolving and complex technological environment with the need for clear and sustainable framework of responsibilities and rules to make the most effective use of this powerful software while managing information risks.

Aim

The Council's objectives for this policy are:

- maximise the benefits of the Microsoft 365 environment including but not limited to Teams, SharePoint, OneDrive and Outlook
- manage the legal, compliance and reputational risks
- create and manage effective documents and records necessary for business, regulatory, legal and accountability purposes
- create and manage an effective Intranet which provides high quality, relevant, accurate and up-to-date information to support Council business
- safeguard the Council's data from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care toward the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of data through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to the Council Microsoft 365 Tenant
- all facilities, technologies and services that use Microsoft 365
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council on Microsoft 365
- internal and external processes used to process Council information
- anyone else given access to Microsoft 365, including external collaborators, guests and visitors.

The policy will be communicated to users and relevant external parties.

Mobile and Bring Your Own Device (BYOD)

Outlines the Council’s approach to use of mobile devices and ‘Bring Your Own Device’ (BYOD).

Statement

This policy outlines the Council’s approach to use of mobile devices and ‘bring your own device’ (BYOD) and provides the guiding principles and responsibilities to ensure the Council’s mobile and BYOD objectives are met.

Aim

The Council’s objectives for this policy are:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care toward the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Mobile device management

Outlines the Council's approach to mobile device management (MDM).

Statement

This policy outlines the Council's approach to mobile device management (MDM) and provides the guiding principles and responsibilities to ensure that consistent and appropriate controls are applied to Council owned mobile devices to help mitigate the risks associated with their use.

Aim

The Council's objectives for this policy are:

- safeguard the Council's information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care toward the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Password management

Outlines the Council’s approach to password creation, use and management.

Statement

This policy outlines the Council’s approach to password management. It provides the guiding principles and responsibilities to ensure appropriate use and management of passwords to improve cybersecurity and prevent cyberattacks that rely on weak or reused passwords.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- internal and external processes used to process Council information

The policy will be communicated to users and relevant external parties.

Patch management

Outlines the Council's approach to the patch management of its infrastructure assets.

Statement

This policy outlines the Council's approach to the patch management of its infrastructure assets. It provides the guiding principles and responsibilities to ensure the Council's patch management objectives are met.

Aim

The Council's objectives for this policy are to:

- safeguard the Council's information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care toward the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.
- enforce patch requirements to ensure that all patches or configuration changes are deployed to Council infrastructure assets when a vulnerability is identified.

Scope

This policy applies to:

- all systems and services which connect to the Council network.

The policy will be communicated to users and relevant external parties.

Physical security

Outlines the Council's approach to the physical security of its information technology assets.

Statement

This policy outlines the Council's approach to physical security of its information technology assets and provides the guiding principles and responsibilities to ensure that consistent and appropriate controls are applied to help prevent loss, damage and theft by deterring, delaying or preventing unauthorised physical access.

Aim

The Council's objectives for this policy are:

- safeguard the Council's information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council's duty of care toward the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects
- prevent the loss, damage and theft of information technology assets by deterring, delaying or preventing unauthorised physical access.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council.

The policy will be communicated to users and relevant external parties.

Protective marking

Refer to the Council Records Management Policy and Procedure.

Remote access

Outlines the Council’s approach to remote access to its computing facilities.

Statement

This policy outlines the Council’s approach to remote access to its computing facilities. It provides the guiding principles and responsibilities to ensure the Council’s remote access objectives are met.

Aim

The Council’s objectives for this policy are to:

- safeguard the Council’s information from security threats that could have an adverse effect on its operations or reputation
- fulfil the Council’s duty of care and legislative responsibilities in relation to the information with which it has been entrusted
- protect the confidentiality, integrity, availability and value of information through the pragmatic use of controls to prevent, or reduce, undesired effects.

Scope

This policy is applicable across the Council and applies to:

- all individuals who have access to Council information and technologies
- all facilities, technologies, and services that are used to process Council information
- all information processed, accessed, shared, manipulated, or stored (in any format) by the Council pursuant to its operational activities
- internal and external processes used to process Council information
- external parties that provide information processing services to the Council
- access to cloud based systems running Council functions or providing services procured by the Council.

The policy will be communicated to users and relevant external parties.

Removable media

Not yet applicable/developed.

Risk management

Not yet applicable/developed.

Secure data deletion/destruction

Refer to the Council Records Management Policy and Procedure.

Secure development

Not yet applicable/developed.

Software assurance

Not yet applicable/developed.

Staff training

Refer to the Council HR Employee Learning and Development Policy.

Supplier management

Refer to the Council Procurement Policy and Procedures